



[Subscribe](#) (Full Service) [Register](#) (Limited Service, Free) [Login](#)

Search: ☒ The ACM Digital Library ☐ The Guide

SEARCH

THE ACM DIGITAL LIBRARY

[Feedback](#)

(((((((media))) and (key))) and (title))) and (block))) and (server))) and (encrypt or cipher or scramble)) and (decrypt or decipher or desramble)
Published before December 2004
Terms used:
media key title block server encrypt cipher scramble decrypt decipher desramble Found **9** of **21** searched out of **255,080**.

Sort
results
by

relevance

Display
results

expanded form



[Save](#) [Refine](#)

[results](#)

[to a](#)

[Binder](#)

these

results

with

[Advanced](#)

[Search](#)



Open
results
in a new
window

Try this

search

in [The](#)

[ACM](#)

[Guide](#)

Results 1 - 9 of 9

1 [Key-assignment strategies for CPPM](#)



André Adelsbach, Jörg Schwenk

September 2004 MM&Sec '04: Proceedings of the 2004 workshop on Multimedia and security

Publisher: ACM

Full text available: Pdf (454.53 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 4, Downloads (12 Months): 26, Citation Count: 0

CSS, the first system to protect multimedia content on the new DVD medium failed badly, because both its encryption algorithm and its key management could easily be broken. A new industry initiative, the 4C Entity, LLC (founded by IBM, Intel, Matsushita ...

Keyw ords: CPPM, content protection, device revocation, key-assignment, key-management

2 The architecture and performance of security protocols in the ensemble group communication system: Using diamonds to guard the castle



August ACM Transactions on Information and System Security (TISSEC),
2001 Volume 4 Issue 3

Publisher: ACM

Full text available: Pdf (418.73 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#),
[index terms](#), [review](#)

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 107, Citation Count: 7

Ensemble is a Group Communication System built at Cornell and the Hebrew universities. It allows processes to create *process groups* within which scalable reliable fifo-ordered multicast and point-to-point communication are supported. The system ...

Keyw ords: Group communication, security

3 Just fast keying: Key agreement in a hostile internet



William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, Omer Reingold

May ACM Transactions on Information and System Security (TISSEC),
2004 Volume 7 Issue 2

Publisher: ACM

Full text available: Pdf (324.39 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#),
[index terms](#)

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 138, Citation Count: 5

We describe Just Fast Keying (JFK), a new key-exchange protocol, primarily designed for use in the IP security architecture. It is simple, efficient, and secure; we sketch a proof of the latter property. JFK also has a number of novel engineering parameters ...

Keyw ords: Cryptography, denial-of-service attacks

4 PocketLens: Toward a personal recommender system



Bradley N. Miller, Joseph A. Konstan, John Riedl

July ACM Transactions on Information Systems (TOIS), Volume 22 Issue 3
2004

Publisher: ACM

Full text available: Pdf (1.10 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 51, Downloads (12 Months): 383, Citation Count: 7

Recommender systems using collaborative filtering are a popular technique for reducing information overload and finding products to purchase. One limitation of current recommenders is that they are not portable. They can only run on large computers connected ...

Keyw ords: Collaborative Filtering, Peer-to-Peer Networking, Privacy, Recommender Systems


5 Rethinking the design of the Internet: the end-to-end arguments vs. the brave new world



Marjory S. Blumenthal, David D. Clark

August ACM Transactions on Internet Technology (TOIT), Volume 1 Issue 1 2001

Publisher: ACM

Full text available:  Pdf (176.33 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 130, Downloads (12 Months): 752, Citation Count: 27

This article looks at the Internet and the changing set of requirements for the Internet as it becomes more commercial, more oriented toward the consumer, and used for a wider set of purposes. We discuss a set of principles that have guided the design ...


Keyw ords: ISP, Internet, end-to-end argument

6 Optimizing the energy consumed by secure wireless sessions: wireless transport layer security case study

Ramesh Karri, Piyush Mishra

April Mobile Networks and Applications, Volume 8 Issue 2 2003

Publisher: Kluwer Academic Publishers

Full text available:  Pdf (151.69 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 67, Citation Count: 4

In this paper we identified the various sources of energy consumption during the setup, operation and tear down of a secure wireless session by considering the wireless transport layer security protocol. Our analysis showed that data transfers during ...

Keyw ords: WTLS, energy-efficient, mobile, secure session, security, wireless

7 Internet security: firewalls and beyond



Rolf Oppliger

May 1997 Communications of the ACM, Volume 40 Issue 5

Publisher: ACM

Full text available: Pdf (339.15 KB) Additional Information: [full citation](#), [references](#), [cited by](#), [index terms](#), [review](#)

Bibliometrics: Downloads (6 Weeks): 54, Downloads (12 Months): 604, Citation Count: 11

8 Practical byzantine fault tolerance and proactive recovery



Miguel Castro, Barbara Liskov

November 2002 ACM Transactions on Computer Systems (TOCS), Volume 20 Issue 4

Publisher: ACM

Full text available: Pdf (1.63 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#), [review](#)

Bibliometrics: Downloads (6 Weeks): 61, Downloads (12 Months): 360, Citation Count: 25

Our growing reliance on online services accessible on the Internet demands highly available systems that provide correct service without interruptions. Software bugs, operator mistakes, and malicious attacks are a major cause of service interruptions ...

Keyw ords: Byzantine fault tolerance, asynchronous systems, proactive recovery, state machine replication, state transfer

9 Secure audit logs to support computer forensics



Bruce Schneier, John Kelsey

May 1999 ACM Transactions on Information and System Security (TISSEC), Volume 2 Issue 2

Publisher: ACM

Full text available: Pdf (125.50 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#), [review](#)

Bibliometrics: Downloads (6 Weeks): 34, Downloads (12 Months): 313, Citation Count: 19

In many real-world applications, sensitive information must be kept it log files on an untrusted machine. In the event that an attacker captures this machine, we would like to guarantee that he will gain little or no information from the log files and ...

Keyw ords: audit logs, auditing, authentication, computer forensics, hash chains, intrusion detection

Results 1 - 9 of 9

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2008 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)